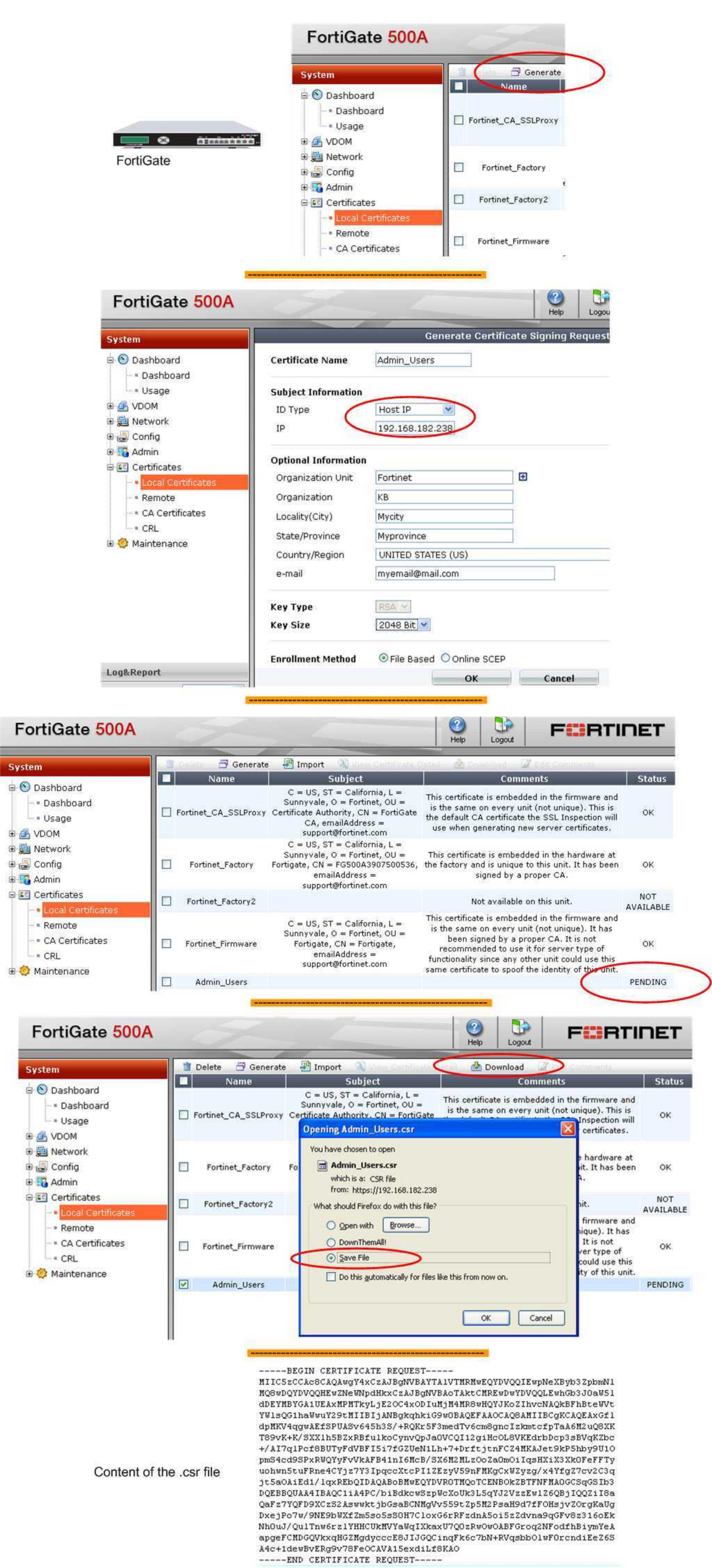
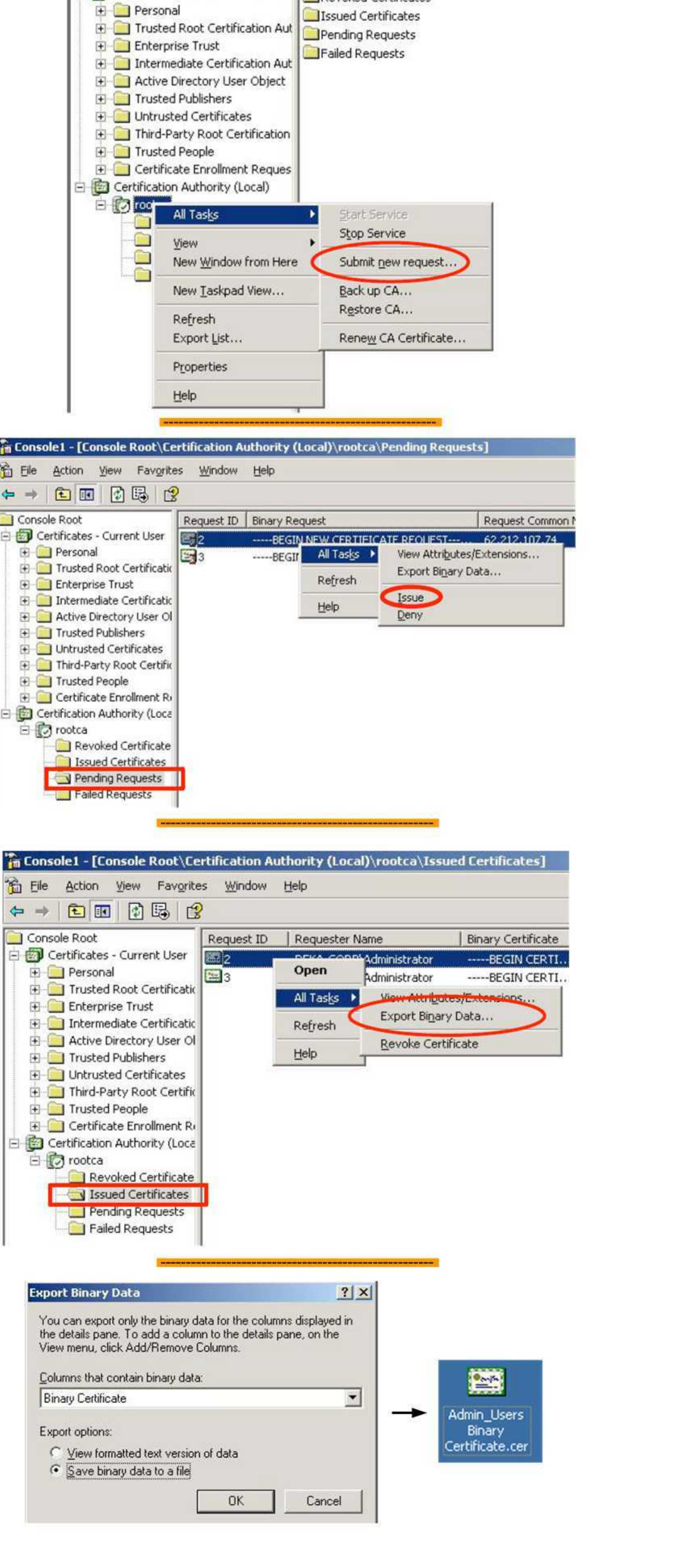
1 – Generate a Certificate Signing Request from the FortiGate Web User Interface

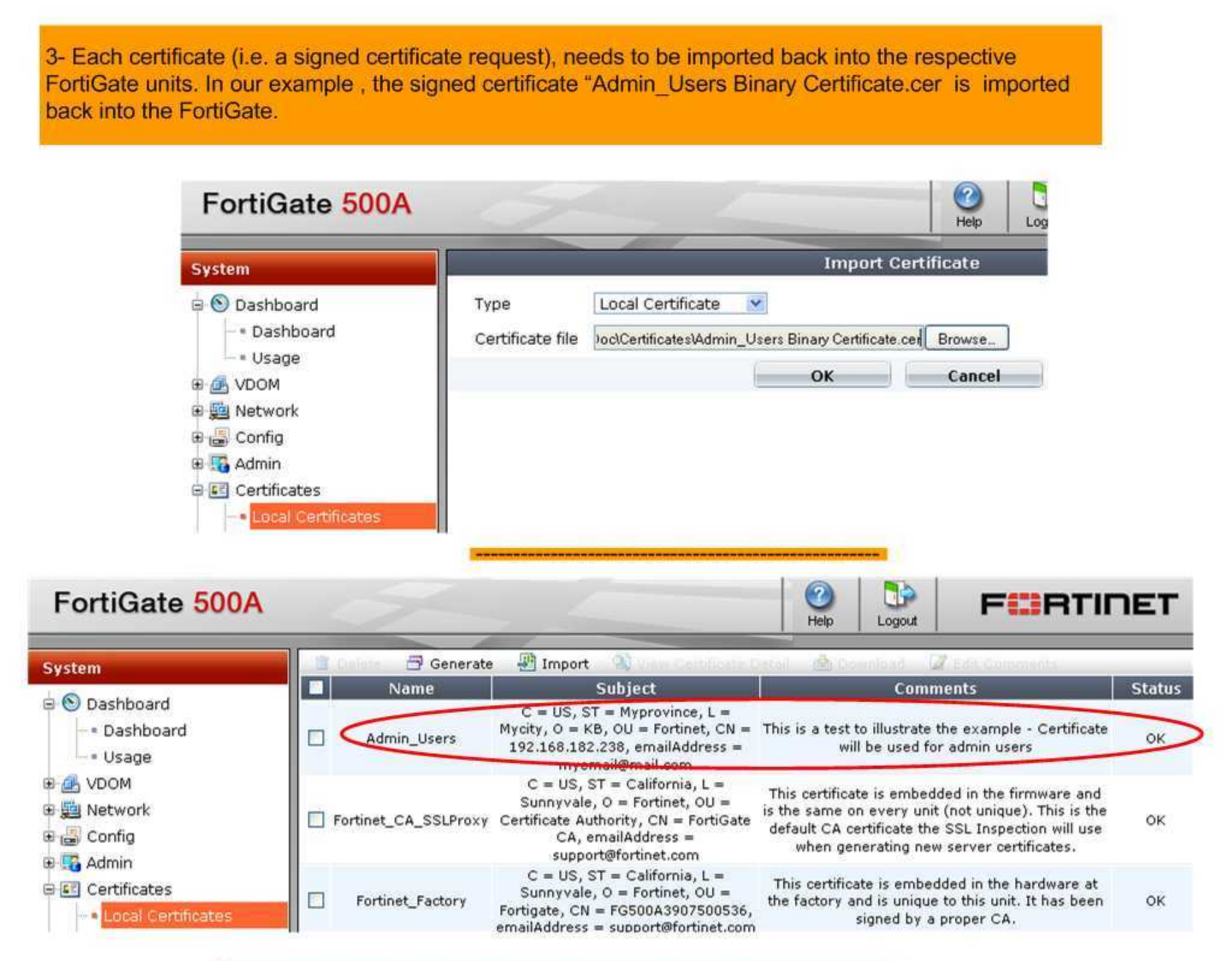


Content of the .csr file

-----BEGIN CERTIFICATE REQUEST-----
MIIC5zCCAc8CAQAwgY4xCzAJBgNVBAYTA1VTMRMwEQYDVQQIEwpNeXByb3ZpbmNl
MQ8wDQYDVQQHEwZNeWNpdHkxCzAJBgNVBAoTAktCMREwDwYDVQQLEwhGb3J0aW51
dDEYMBYGA1UEAxMPMTkyLjE2OC4xODIuMjM4MR8wHQYJKoZIhvcNAQkBFhBteWVt
YWlsQG1haWwuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxGf1
dpMKV4qgwAEfSPUASv645h3S/+RQKr5F3medTv6cm8gncIzkmtcfpTaA6M2uQ8XK
T89vK+K/SXX1h5BZxRBfulkoCynvQpJa0VCQI12giHcOL8VKEdrbDcp3sBVqKZbc
+/AI7q1Pcf8BUTyFdVBFI5i7fGZUeN1Lh+7+DrftjtnFCZ4MKAJet9kP5hby9U1O
pmS4cd9SPxRWQYyFvVkAFB41nI6McB/SX6M2MLzOoZaOmOiIqsHXiX3XkOFeFFTy
uohwn5tuFRne4CYjz7Y3IpqccXtcPI1ZEzyV59nFMKgCxWZyzg/x4YfgZ7cv2C3q
jt5aOAiEd1/1qxREbQIDAQABoBMwEQYDVR0TMQoTCENBOkZBTFNFMA0GCSqGSIb3
DQEBBQUAA4IBAQC1iA4PC/biBdkcwSzpWcXoUk3L5qYJ2VzzEw1Z6QBjIQQZiI8a
QaFz7YQFD9XCzS2AswwktjbGsaBCNMgVv559tZp5M2PsaH9d7fFOHsjvZOrgKaUg
DxejPo7w/9NE9bWXfZm5so5sSOH7CloxG6rRFzdnA5oi5zZdvna9qGFv8z316oEk
NhOuJ/QulTnw6rz1YHHCUkMVYaWqIXkaxU7QOzRwOwOABFGroq2NFodfhBiymYeA
apgeFCMDGQVkxqHGZMgdycccE8JIJGQCinqFk6c7bN+RVqsbbO1wFOrcndiEeZ6S
A4c+1dewBvERg9v78FeOCAVA15exdiLf8KAO
-----END CERTIFICATE REQUEST-----



3- Each certificate (i.e. a signed certificate request), needs to be imported back into the respective FortiGate units. In our example , the signed certificate "Admin_Users Binary Certificate.cer is imported back into the FortiGate.

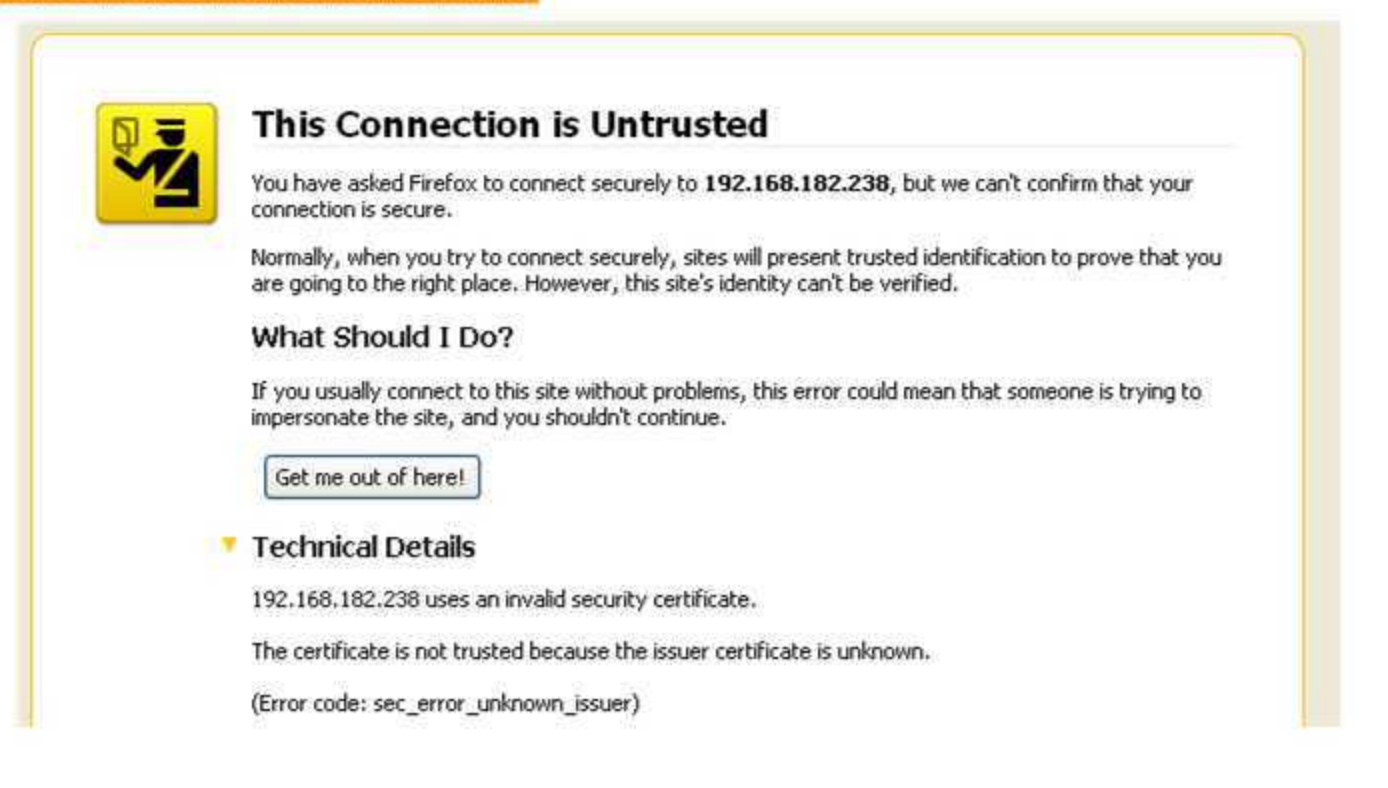


4 - Change the FortiGate's Certificate to use for admin connection

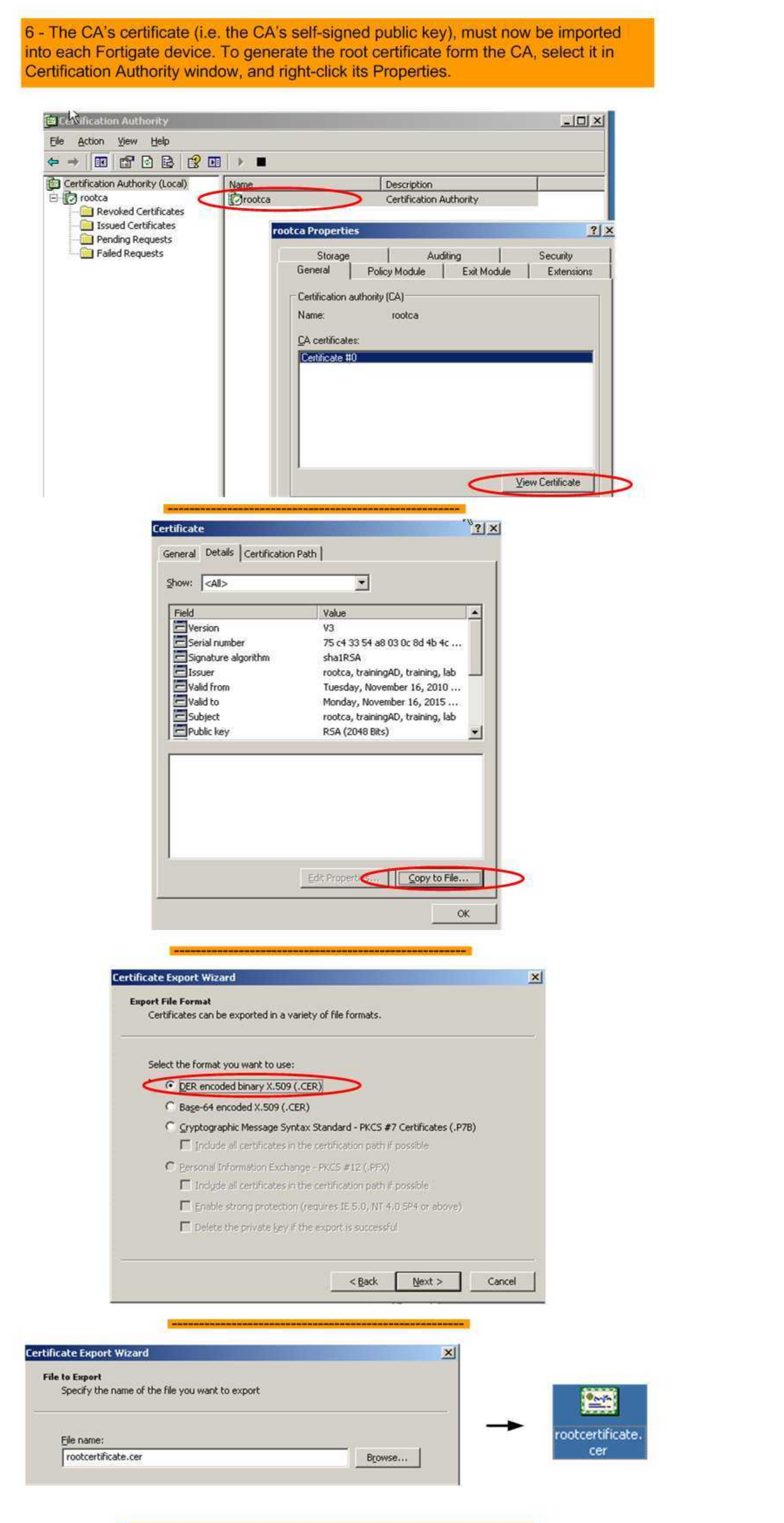
```
MASTER (global) # sho system global
config system global
    set admin-server-cert "Admin_Users"
    set hostname "MASTER"
    set optimize antivirus
    set vdom-admin enable
end

MASTER (global) #
```

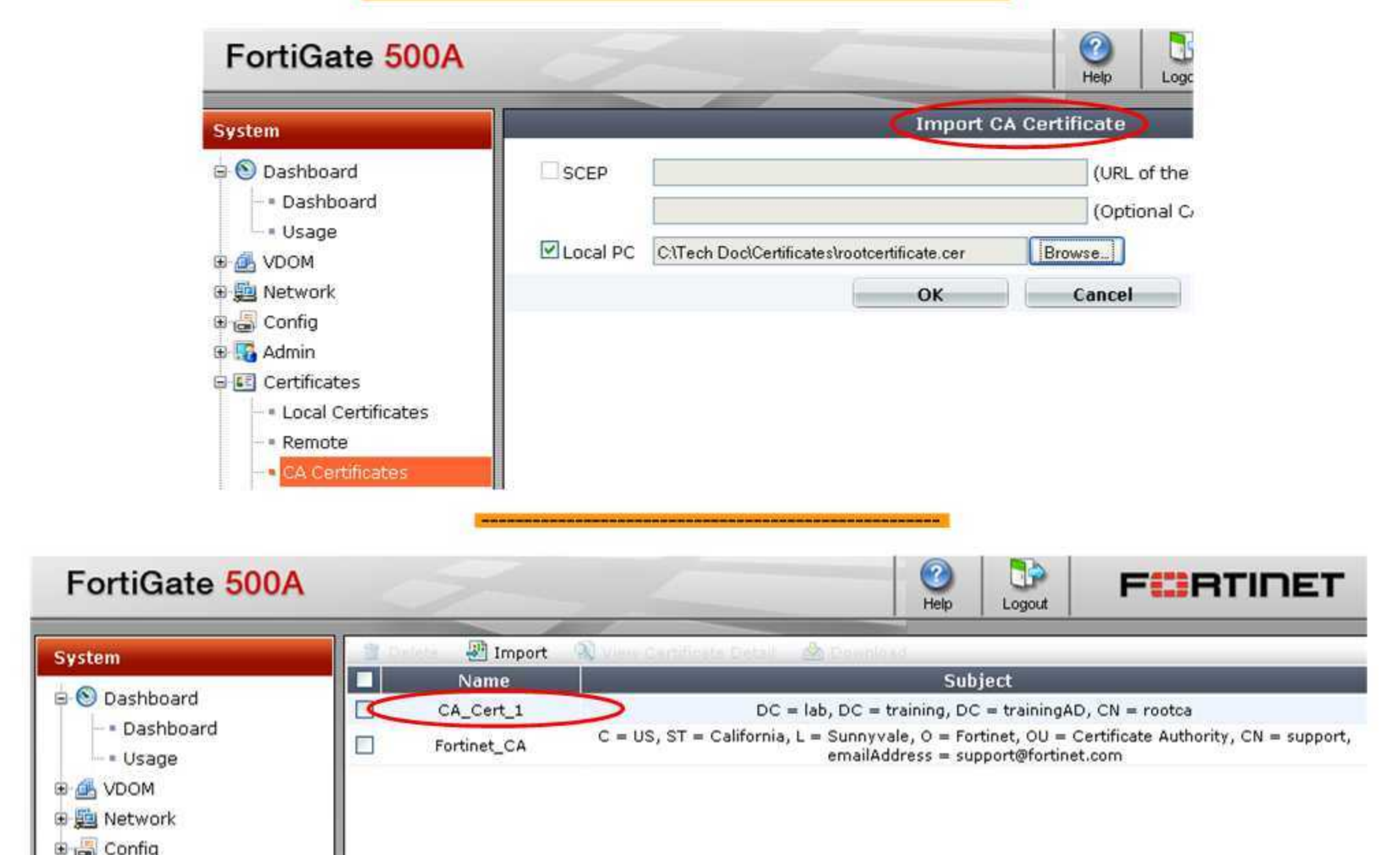
5 - But we see that trying to connect again will still hit a security issue. That is because the browser does not know the root certificate yet



6 - The CA's certificate (i.e. the CA's self-signed public key), must now be imported into each Fortigate device. To generate the root certificate form the CA, select it in Certification Authority window, and right-click its Properties.

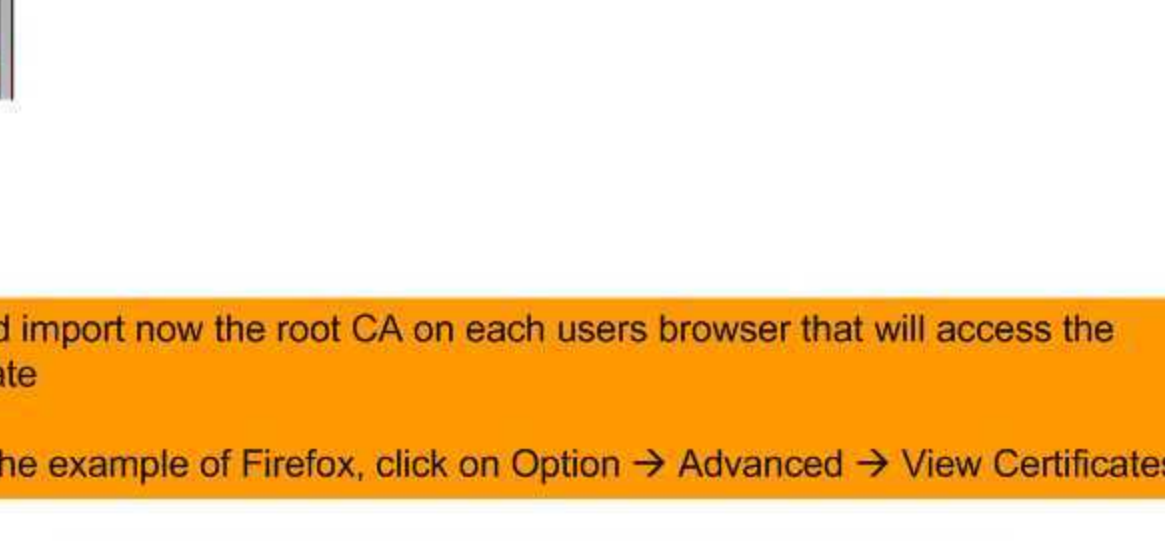


7 - This now needs to be imported into the Fortigate.

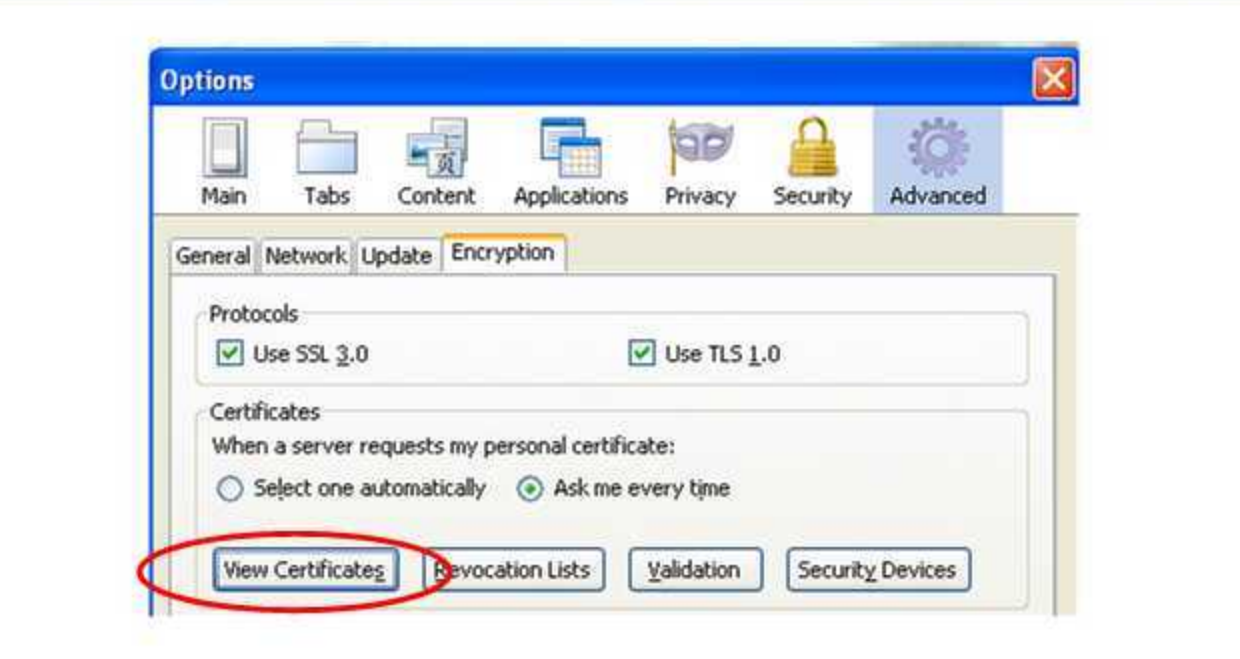


8 – And import now the root CA on each users browser that will access the FortiGate

8.1 In the example of Firefox, click on Option → Advanced → View Certificates

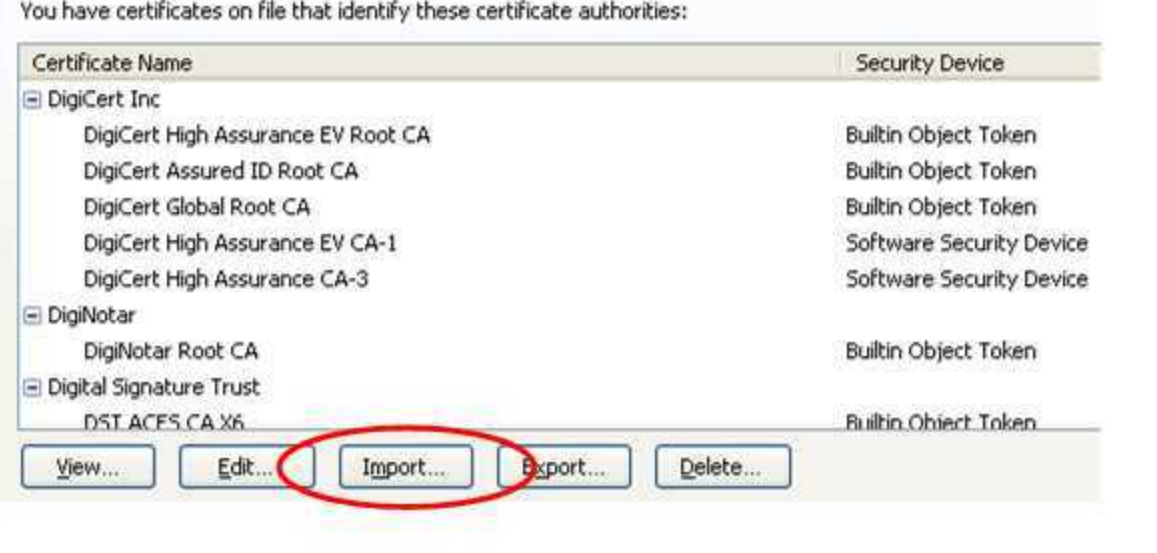


8.2 → Import



8.3 – Select the root CA

8.4 – Select the purpose of using to use this root CA



9 – The HTTPS session is now opening without any security warning